Jurnal Masyarakat Informatika, 15(1), 2024
DOI:10.14710/jmasif.15.1.60836
ISSN: 2777-0648

Kriptografi Teks Berbasis Algoritma Substitusi Vigenere Cipher 8 Bit

Nida Aulia Karima*, Ade Nurul Aisyah, Hercio Venceslau Silla, L. Budi Handoko, Ramadhan Rakhmat Sani
Fakultas Ilmu Komputer, Universitas Dian Nuswantoro, Semarang, Indonesia
* *Corresponding author: 111202113495@mhs.dinus.ac.id*

Abstrak
Vigenere Cipher merupakan salah satu algoritma kriptografi klasik dalam dunia kriptografi. Penelitian ini berfokus pada penggunaan metode Vigenere Cipher dan implementasinya dalam mengamankan sebuah teks pesan berbentuk ASCII. Penelitian ini menggunakan empat metode pengujian yaitu, Avalanche Effect, Character Error Rate (CER), Bit Error Rate (BER), dan Entropi. Hasil pengujian mendapatkan bahwa nilai Avalanche Effect yang dihasilkan rata-rata berada pada angka 50% ke atas, artinya diperoleh nilai Avalanche Effect yang baik. Selain itu, CER dan BER yang dihasilkan bernilai 0, artinya tidak terjadi kesalahan selama proses enkripsi. Nilai Entropi yang dihasilkan juga meningkat seiring dengan panjang plaintext yang digunakan dan juga dipengaruhi penggunaan ASCII 256 berupa huruf, angka, dan simbol.

Kata kunci : *Kriptografi, Vigenere Cipher, ASCII, Avalanche Effect, Entropi*

Abstract
Vigenere Cipher is one of the classic cryptographic algorithms in the world of cryptography. This research focuses on the use of the Vigenere Cipher method and its implementation in securing an ASCII message text. This research uses four testing methods namely, Avalanche Effect, Character Error Rate (CER), Bit Error Rate (BER), and Entropy. The test results found that the Avalanche Effect value produced on average was at 50% and above, meaning that a good Avalanche Effect value was obtained. In addition, the resulting CER and BER are 0, meaning that no errors occurred during the encryption process. The resulting Entropy value also increases along with the length of the plaintext used and is also influenced by the use of ASCII 256 in the form of letters, numbers, and symbols.

Keywords : *Cryptography, Vigenere Cipher, ASCII, Avalanche Effect, Entropy*

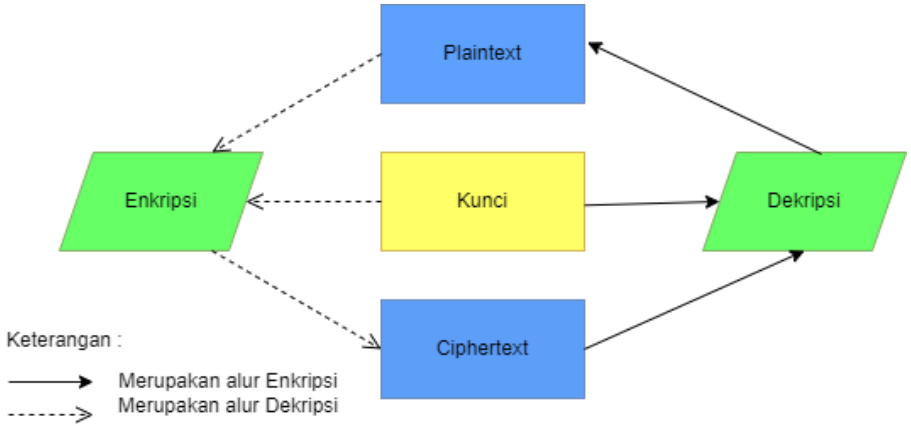
1 Pendahuluan

Cybercrime merupakan sebuah kejahatan yang dilakukan di dunia maya dengan menggunakan teknologi komputer sebagai alat utama target kejahatan. Salah satu bentuk cybercrime adalah pencurian data pribadi seseorang, dengan data pribadi seseorang pihak yang tidak bertanggung jawab dapat menggunakanya untuk berbagai kejahatan yang lain seperti, penipuan online dengan mengatasnamakan nama korban, kerugian financial yang mana pihak yang tidak bertanggung jawab mengetahui kata sandi pin atm ataupun dompet digital korban dan reputasi korban menjadi rusak akibat ada penyalahgunaan akun sosial media yang dikendalikan pihak yang tidak bertanggung jawab. Oleh karena itu diperlukan keamanan untuk melindungi ataupun menjaga kerahasiaan data yang dimiliki

Received: 20 December 2023; Revised: 9 May 2024; Accepted: 10 May 2024; Published: 31 May 2024.

[1]–[3], agar pihak yang tidak bertanggung jawab tidak dapat mengambil alih data pribadi melalui teknik kriptografi.

Kriptografi [4]–[8] adalah bidang ilmu yang berkaitan dengan teknik untuk menjaga keamanan data dan informasi seperti menjaga kerahasiaan suatu data, integrasi data, autentikasi, dan non repudiasi. Data harus dijaga kerahasiaanya agar pihak yang tidak bertanggung jawab tidak dapat mengakses. Kriptografi tidak hanya berfokus pada mengamankan data. Namun, mempelajari juga suatu pola dimana membuat suatu informasi yang sulit untuk dibaca [9]–[13]. Sehingga hanya seseorang yang telah diberikan hak saja yang dapat mengaksesnya. Karena tujuan dari kriptografi adalah mengubah informasi dengan pesan yang mudah dipahami semua orang (plaintext) menjadi bentuk yang tidak mudah dipahami atau sulit untuk dibaca(ciphertext) [14]–[16]. Secara umum terdapat dua proses utama dalam kriptografi yaitu enkripsi dan dekripsi. Proses enkripsi terjadi antara tidak lain yaitu untuk mengubah suatu bentuk pesan asli menjadi sebuah sandi, dan proses dekripsi yaitu proses yang mengubah suatu sandi menjadi sebuah pesan asli. Kedua proses tersebut minimal membutuhkan sebuah kunci. Gambar 1 merupakan gambaran umum dari kedua proses dalam kriptografi.



Gambar 1 Enkripsi dan Dekripsi Berbasis Kunci Simetris

Kriptografi juga memiliki banyak bentuk metode algoritma dalam penerapanya, sesuai studi kasus yang dibutuhkan. Kunci yang digunakan untuk melakukan proses enkripsi dan dekripsi sekaligus adalah kriptografi simetris. Salah satu kriptografi klasik yang populer adalah Vigenere Cipher. Algoritma Vigenere Cipher juga merupakan sebuah algoritma kriptografi substitusi [17]. Kriptografi substitusi merupakan teknik yang merubah plaintext dengan ciphertext berdasarkan kunci. Selain mudah dalam pengimplementasianya juga memiliki kelebihan antara lain yaitu Vigenere Cipher termasuk kedalam polialfabetik cipher yang berarti setiap huruf pada plaintext dapat dienkripsikan menjadi huruf yang berbeda dalam ciphertext (berfokus pada frekuensi huruf) [16], [18]–[20], kunci yang panjang dan berubah-ubah meningkatkan keamanan karena pola enkripsi yang dihasilkan menjadi lebih sulit untuk diprediksi, dengan menggunakan kunci yang panjang dan berubah-ubah vigenere cipher mampu mengatasi kelemahan utama Caesar Cipher, yaitu pola yang konsisten dalam pengaplikasian enkripsinya.

Tujuan dari metode Vigenere Cipher dalam penggunaan teks ASCII membuat kunci yang dihasilkan Vigenere Cipher menjadi beragam karena mencakup huruf, angka, dan karakter khusus dalam pengimplementasianya. Penggunaan teks ASCII juga meningkatkan keamanan yang akan dihasilkan. Dalam penelitian ini, telah dilakukan pengujian dengan menggunakan metode Avalanche

Effect, Bit Error Rate dan Character Error Rate, yang mana dari pengujian tersebut Avalanche Effect bertujuan dalam mengukur seberapa besar perubahan pada input (plaintext) dan output (ciphertext). Bit Error Rate bertujuan dalam mengukur seberapa banyak bit yang dienkripsi yang tidak sesuai dengan bit yang seharusnya ada, dan Character Error Rate bertujuan dalam mengukur seberapa banyak karakter yang dihasilkan oleh proses enkripsi yang tidak cocok dengan karakter seharusnya.

2 Metode Penelitian

2.1 Kriptografi

Kriptografi atau dalam Bahasa Inggris disebut dengan Cryptography berasal dari Bahasa Yunani kuno yang terdiri dari dua kata yaitu “cryptos” yang memiliki arti rahasia dan “graphein” yang memiliki arti menulis. Sehingga, kriptografi dapat diartikan sebagai suatu teknik menulis rahasia [13], [21]. Kriptografi merupakan cabang ilmu yang dikembangkan untuk mempelajari tentang penyandian suatu informasi atau data dengan tujuan untuk menjaga kerahasiaan dan keamanan suatu informasi atau data tersebut. Terdapat beberapa komponen penting dalam kriptografi, yaitu plaintext (pesan yang dapat dibaca), ciphertext (pesan sandi atau pesan acak yang tidak dapat dibaca), dan key (kunci untuk melakukan teknik kriptografi).

2.2 Kriptografi dengan Metode Substitusi

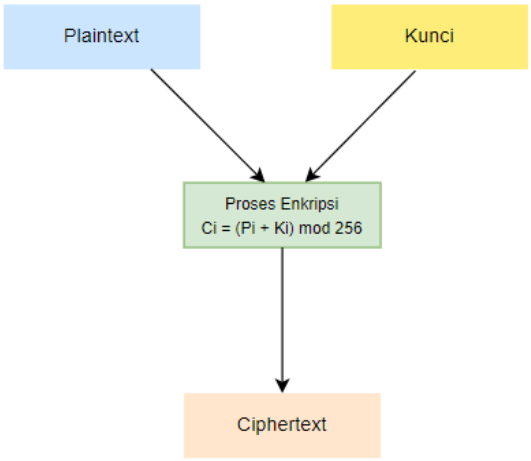
Kriptografi adalah bidang ilmu yang berkaitan dengan teknik untuk menjaga keamanan data dan informasi seperti menjaga kerahasiaan suatu data, integrasi data, autentikasi, dan non repudiasi. Jaman dulu menggunakan kriptografi klasik. Kriptografi klasik umumnya menggunakan metode subtitusi dan metode transposisi. Metode substitusi merupakan teknik yang mengubah plaintext dengan ciphertext berdasarkan kunci [12], [22]. *American Standard Code for Information Interchange (ASCII)* merupakan representasi numerik dari suatu karakter yang menjadi acuan untuk karakter dalam komunikasi yang mewakili huruf sampai simbol-simbol, saat melakukan pengkodean karakter yang sering digunakan dalam proses enkripsi [23].

2.3 Alur Enkripsi dan Dekripsi

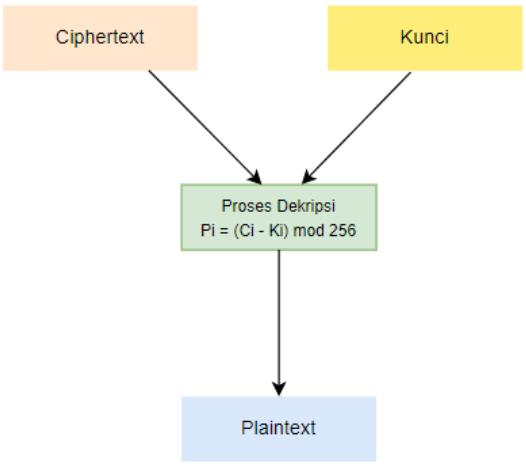
Berdasarkan Gambar 3, alur proses enkripsi terjadi ketika diinputkan sebuah plaintext atau teks asli dengan kunci/key, lalu dilakukan proses enkripsi atau proses mengkonversi sebuah teks ke dalam bentuk kode atau sandi, maka akan menghasilkan sebuah teks bersandi (ciphertext). Kemudian proses dekripsi terjadi ketika diinputkan ciphertext atau teks bersandi dengan menggunakan kunci/key yang sama, kemudian dilakukan proses dekripsi yaitu proses mengkonversi sandi atau kode ke dalam bentuk text asli, maka akan kembali menghasilkan text asli (plaintext), sesuai dengan Gambar 4.

DC	AC	AS+UC	DC	All	DC	All	DC	All	DC	AC	UC	EA	DC	AC	UC	EA	DC	AC	UC	EA	DC	AC	UC	EA
NUL	NUL	NUL	32	SP	64	@	96	`	128	€	xxx	Ç	160		nbsp	á	192	À	À	└	224	à	à	Ó
1	☺	SOH	33	!	65	A	97	a	129		xxx	ü	161	¡	¡	í	193	Á	Á	┴	225	á	á	ß
2	☻	STX	34	"	66	B	98	b	130	‚	BPH	é	162	¢	¢	ó	194	Â	Â	┬	226	â	â	Ô
3	♥	ETX	35	#	67	C	99	c	131	ƒ	NBH	â	163	£	£	ú	195	Ã	Ã	├	227	ã	ã	Ò
4	♦	EOT	36	$	68	D	100	d	132	„	IND	ä	164	¤	¤	ñ	196	Ä	Ä	─	228	ä	ä	õ
5	♣	ENQ	37	%	69	E	101	e	133	…	NEL	à	165	¥	¥	Ñ	197	Å	Å	┼	229	å	å	Õ
6	♠	ACK	38	&	70	F	102	f	134	†	SSA	å	166	¦	¦	ª	198	Æ	Æ	ã	230	æ	æ	µ
7	•	BEL	39	'	71	G	103	g	135	‡	ESA	ç	167	§	§	º	199	Ç	Ç	Ã	231	ç	ç	þ
8	◘	BS	40	(	72	H	104	h	136	ˆ	HTS	ê	168	¨	¨	¿	200	È	È	╚	232	è	è	Þ
9	○	HT	41	)	73	I	105	i	137	‰	HTJ	ë	169	©	©	®	201	É	É	╔	233	é	é	Ú
10	◙	LF	42	*	74	J	106	j	138	Š	VTS	è	170	ª	ª	¬	202	Ê	Ê	╩	234	ê	ê	Û
11	♂	VT	43	+	75	K	107	k	139	‹	PLD	ï	171	«	«	½	203	Ë	Ë	╦	235	ë	ë	Ù
12	♀	FF	44	,	76	L	108	l	140	Œ	PLU	î	172	¬	¬	¼	204	Ì	Ì	╠	236	ì	ì	ý
13	♪	CR	45	-	77	M	109	m	141		RI	ì	173	-	-	¡	205	Í	Í	═	237	í	í	Ý
14	♫	SO	46	.	78	N	110	n	142	Ž	SS2	Ä	174	®	®	«	206	Î	Î	╬	238	î	î	¯
15	☼	SI	47	/	79	O	111	o	143		SS3	Å	175	¯	¯	»	207	Ï	Ï	¤	239	ï	ï	´
16	►	DLE	48	0	80	P	112	p	144		DSC	É	176	°	°	░	208	Đ	Đ	ð	240	ð	ð	
17	◄	DC1	49	1	81	Q	113	q	145	‘	PU1	æ	177	±	±	▒	209	Ñ	Ñ	Đ	241	ñ	ñ	±
18	↕	DC2	50	2	82	R	114	r	146	’	PU2	Æ	178	²	²	▓	210	Ò	Ò	Ê	242	ò	ò	‗
19	‼	DC3	51	3	83	S	115	s	147	“	STS	ô	179	³	³	│	211	Ó	Ó	Ë	243	ó	ó	¾
20	¶	DC4	52	4	84	T	116	t	148	”	CCH	ö	180	´	´	┤	212	Ô	Ô	È	244	ô	ô	¶
21	§	NAK	53	5	85	U	117	u	149	•	MW	ò	181	µ	µ	Á	213	Õ	Õ	ı	245	õ	õ	§
22	▬	SYN	54	6	86	V	118	v	150	–	SPA	û	182	¶	¶	Â	214	Ö	Ö	Í	246	ö	ö	÷
23	↨	ETB	55	7	87	W	119	w	151	—	EPA	ù	183	·	·	À	215	×	×	Î	247	÷	÷	¸
24	↑	CAN	56	8	88	X	120	x	152	˜	SOS	ÿ	184	¸	¸	©	216	Ø	Ø	Ï	248	ø	ø	°
25	↓	EM	57	9	89	Y	121	y	153	™	xxx	Ö	185	¹	¹	╣	217	Ù	Ù	┘	249	ù	ù	¨
26	→	SUB	58	:	90	Z	122	z	154	š	SCI	Ü	186	º	º	║	218	Ú	Ú	┌	250	ú	ú	·
27	←	ESC	59	;	91	[	123	{	155	›	CSI	ø	187	»	»	╗	219	Û	Û	█	251	û	û	¹
28	∟	FS	60	<	92	\	124	|	156	œ	ST	£	188	¼	¼	╝	220	Ü	Ü	▄	252	ü	ü	³
29	↔	GS	61	=	93	]	125	}	157		OSC	Ø	189	½	½	¢	221	Ý	Ý	¦	253	ý	ý	²
30	▲	RS	62	>	94	^	126	~	158	ž	PM	×	190	¾	¾	¥	222	Þ	Þ	▌	254	þ	þ	■
31	▼	US	63	?	95	_	127	DEL	159	Ÿ	APC	ƒ	191	¿	¿	┐	223	ß	ß	▀	255	ÿ	ÿ	nbsp

Gambar 2 Representasi Kode ASCII 256



Gambar 3 Alur Proses Enkripsi



Gambar 4 Alur Konsep Dekripsi

2.4 Vigenere Cipher

Vigenere Cipher merupakan salah satu algoritma kriptografi klasik yang dipublikasikan oleh Blaise de Vigenere, seorang diplomat sekaligus kriptologis yang berasal dari Perancis, pada abad 16 [16], [24]. Vigenere cipher adalah sandi substitusi polialfabetik yang terdiri dari seperangkat aturan substitusi monoalfabetik dari sandi Caesar dengan pergeseran 0-25 [6]. Dalam proses enkripsi, vigenere cipher menggunakan pola pergeseran dan dapat dicari menggunakan tabula recta [25], seperti pada Gambar 5. Selain itu, proses enkripsi dan dekripsi pada vigenere cipher dapat menggunakan persamaan (1) dan persamaan (2). Proses enkripsi dapat dilihat pada Gambar 4.

$$\text{Enkripsi} : Ci = (Pi + Ki)\ mod\ 26 \quad (1)$$

$$\text{Dekripsi} : Pi = (Ci - Ki)\ mod\ 26 \quad (2)$$

Keterangan :

Ci = Ciphertext dari C_0 sampai C_n

Pi = Plaintext dari P_0 sampai P_n

Ki = Key dari K_0 sampai K_n

Plaintext	D	I	N	U	S
Kunci/Key	O	K	E	O	K
Ciphertext	R	S	R	I	C

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

Gambar 5 Proses Enkripsi dengan Tabula Recta

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Enkripsi : $Ci = (Pi + Ki)\ mod\ 26$

Plaintext	: D	I	N	U	S
Kunci/Key	: O	K	E	O	K

Gambar 6 Proses Enkripsi dengan Persamaan

Berdasarkan Gambar 6, perhitungan manual metode vigenere cipher untuk mencari ciphertext yang dihasilkan dari plaintext “DINUS” dan kunci “OKE” dapat dilakukan dengan persamaan (1). Sehingga proses enkripsi yang didapat adalah sebagai berikut :

Proses Enkripsi:

C1 = (D + O) mod 26 = (3 + 14) mod 26 = 17 mod 26 = 17 → R

C2 = (I + K) mod 26 = (8 + 10) mod 26 = 18 mod 26 = 18 → S

C3 = (N + E) mod 26 = (13 + 4) mod 26 = 17 mod 26 = 17 → R

C4 = (U + O) mod 26 = (20 + 14) mod 26 = 34 mod 26 = 8 → I

C5 = (S + K) mod 26 = (18 + 10) mod 26 = 28 mod 26 = 2 → C

Ciphertext : R S I R C

Dalam penelitian ini telah digunakan ASCII 256, maka dalam rumus modulo diganti dengan 256, dengan Ci merupakan ciphertext dari C0 sampai dengan Cn, Pi merupakan plaintext dari P0 sampai dengan Pn, dan Ki adalah key/kunci dari K0 sampai dengan Kn [3]. Maka rumus enkripsi dan dekripsi yang digunakan adalah sebagai berikut :

$$\text{Enkripsi : } Ci = (Pi + Ki)\ mod\ 256 \quad (3)$$

$$\text{Dekripsi : } Pi = (Ci - Ki)\ mod\ 256 \quad (4)$$

Misalnya dalam sebuah studi kasus diketahui bahwa “DINUS” adalah sebuah plaintext dan “OKE” adalah kunci, maka berdasarkan rumus diatas proses enkripsinya adalah sebagai berikut :

- $C_1 = (P_1 + K_1) \bmod 256$
  $= (D + O) \bmod 256$
  $= (68 + 79) \bmod 256$
  $= 147$ (“)
- $C_2 = (P_2 + K_2) \bmod 256$
  $= (I + K) \bmod 256$
  $= (73 + 75) \bmod 256$
  $= 148$ (“)
- $C_3 = (P_3 + K_3) \bmod 256$
  $= (N + E) \bmod 256$¤
  $= (78 + 69) \bmod 256$
  $= 147$ (“)
- $C_4 = (P_4 + K_4) \bmod 256$
  $= (U + O) \bmod 256$
  $= (85 + 79) \bmod 256$
  $= 164$ (¤)
- $C_5 = (P_5 + K_5) \bmod 256$
  $= (S + K) \bmod 256$
  $= (83 + 75) \bmod 256$
  $= 158$ (ž)

Ciphertext : “””¤ž

2.5 Avalanche Effect

Avalanche Effect adalah salah satu metode pengujian dalam kriptografi yang menentukan seberapa baik suatu algoritma dengan mencari besar persentase pengubahan pesan pada saat proses enkripsi dilakukan [26], [27]. Hal ini dilakukan dengan melihat rasio antara jumlah bit pada ciphertext yang berubah dan jumlah bit dari plaintext sebelum diubah. Perubahan bit sebesar 45-60% menunjukkan bahwa pengujian Avalanche Effect dianggap baik, dimana 50% adalah hasil yang dianggap baik dalam pengujian [28]. Perhitungan avalanche effect dapat dilihat dalam persamaan (5).

$$AE = \frac{Jumlah\ Perubahan\ Bit}{Jumlah\ Total\ Bit} \times 100\% \quad (5)$$

Jika diketahui dalam sebuah proses enkripsi memiliki jumlah perubahan bit sebesar 16 bit dari total bit pada ciphertext sebesar 40 bit, maka persentase Avalanche Effect adalah sebagai berikut :

$$AE = \frac{16}{40} \times 100\% = 40\%$$

2.6 Bit Error Rate

Bit Error Rate merupakan salah satu metode pengujian dalam kriptografi yang digunakan untuk mencari besar persentase bit yang dilakukan dengan cara membandingkan jumlah bit yang salah dengan total bit pada saat melakukan penyisipan [29]. BER dikatakan baik jika nilainya mendekati 0, yang menyatakan tidak adanya perbedaan antara ciphertext dan plaintext. Perhitungan BER dinyatakan dalam persamaan (6).

$$BER = \frac{Jumlah\ Bit\ Error}{Jumlah\ Total\ Bit} \times 100\% \quad (6)$$

Misalnya terdapat 4 bit yang salah dari total 40 bit, maka diperoleh perhitungan sebagai berikut:

$$BER = \frac{4}{40} \times 100\% = 10\% = 0{,}1$$

2.7 Character Error Rate

Character Error Rate merupakan metode pengujian yang dilakukan dengan cara mencocokan dan membandingkan karakter yang ada pada plaintext dengan plaintext yang diubah atau ditambah. Metode ini berfungsi untuk mengukur besar prosentase tingkat akurasi hasil enkripsi, dimana semakin rendah persentase hasil pengujian maka semakin bagus enkripsi yang dihasilkan [30]. Perhitungan CER dapat dilihat dalam persamaan (7) berikut.

$$CER = \frac{Jumlah\ Karakter\ Berbeda}{Jumlah\ Karakter\ yang\ Dikirim} \times 100\% \quad (7)$$

Jika terdapat 2 karakter yang berbeda dari total karakter yang dikirim sebanyak 40 karakter, maka didapatkan perhitungan sebagai berikut :

$$CER = \frac{2}{40} \times 100\% = 5\% = 0{,}05$$

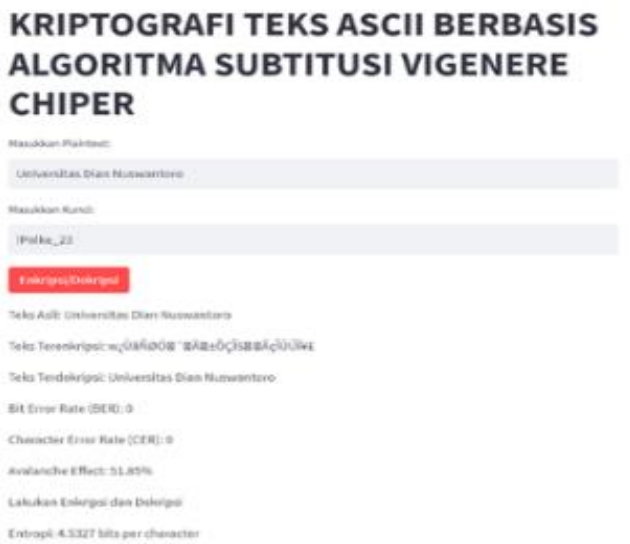
2.8 Entropi

Entropi merupakan sebuah konsep kriptografi yang berfungsi untuk memperkirakan jumlah bit rata-rata dalam pengkodean pesan [11]. Besaran entropi dinyatakan dalam satuan bit. Cara menghitung entropi dituliskan dalam persamaan (8) berikut.

$$He = -\sum_{k=0}^{n} P(k) \log 2(P(k)) \quad (8)$$

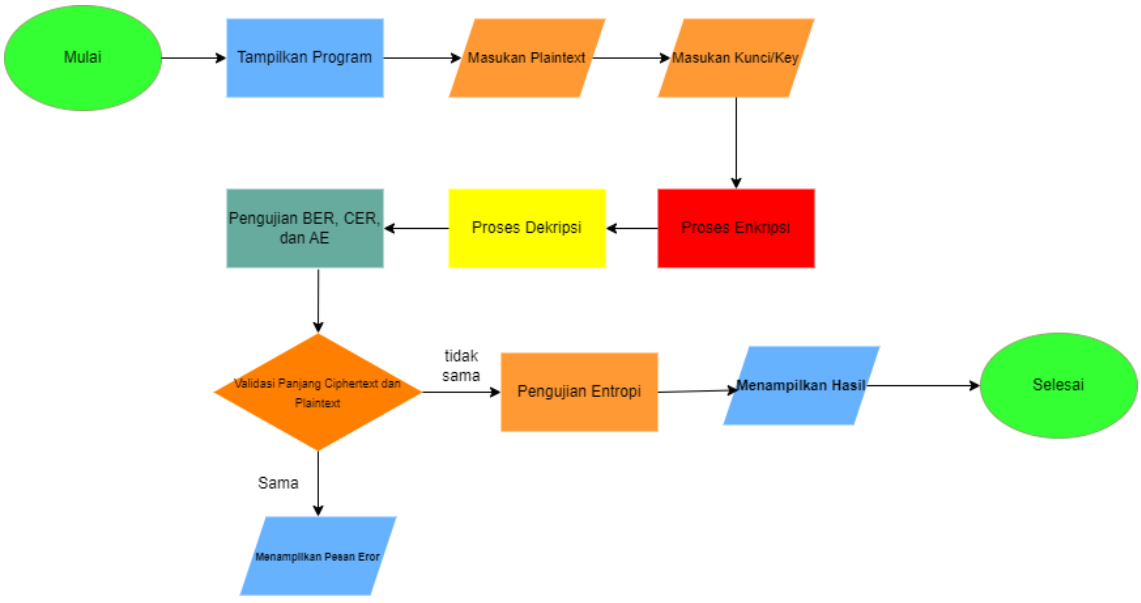
3 Hasil dan Pembahasan

Penelitian ini disusun dengan bahasa pemrograman python dan menggunakan kerangka kerja streamlit untuk menarik skrip python untuk dijalankan dan menampilkan hasilnya di browser. Dan hasil yang akan ditampilkan saat dijalankan seperti pada Gambar 7.



Gambar7 Hasil Keluaran/Output

Gambar 7 menunjukan hasil keluaran ketika memasukkan plaintext dan juga kunci yang hasilnya seperti yang ditunjukkan pada Gambar 8 terdapat teks asli, teks terenkripsi, teks terdekripsi, BER, CER, Avalanche Effect (AE) dan Entropi. Proses yang terjadi dalam sistem ditunjukkan dalam flowchart pada Gambar 8.



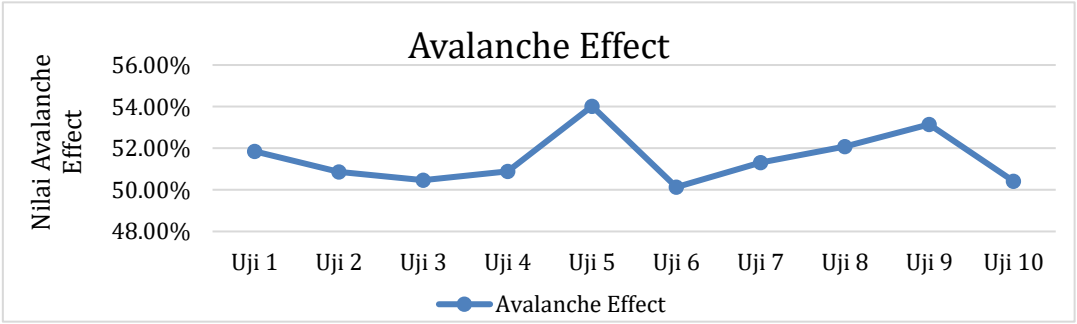
Gambar 7 Flowchart Program

Pada Gambar 8 menjelaskan alur proses yang terjadi pada sistem diawali dengan menampilkan tampilan awal program. Kemudian masukkan plaintext berupa huruf maupun gabungan antara huruf, simbol, dan angka (teks ASCII). Langkah selanjutnya, masukkan teks kunci/ key. Lalu proses enkripsi,

dekripsi dijalankan, kemudian dilanjutkan dengan pengujian BER, CER, AE, dan Entropi. Pada pengujian BER terdapat validasi dimana jika panjang plaintext dan ciphertext tidak sama akan memunculkan pesan error. Namun, jika panjang plaintext dan ciphertext sama, akan lanjut pada proses berikutnya, yaitu pengujian CER dan AE.

Pada proses pengujian CER dan AE juga sama seperti pengujian BER yaitu terdapat validasi jika panjang plaintext dan ciphertext berbeda akan memunculkan pesan error. Namun, jika panjang plaintext dan ciphertext sama maka dilanjutkan pada proses Entropi. Setelah proses Entropi dijalankan, program akan menampilkan hasil berupa plaintext, ciphertext, nilai BER, CER, AE, dan Entropi, kemudian program selesai. Dalam pengujian ini dilakukan 10 kali percobaan dengan jenis pesan berupa plaintext pendek dan sedang. Jenis pesan tersebut berupa huruf saja, gabungan antara huruf dan angka, gabungan antara huruf dan simbol, maupun gabungan antara ketiganya. Pada semua percobaan digunakan kunci yang sama berupa 1 kata yaitu "!Polke_23" yang terdiri dari huruf, angka, dan simbol. Hasil dari pengujian dapat dilihat dari Tabel 1.

Berdasarkan Tabel 1, dapat dilihat bahwa metode vigenere cipher dapat digunakan pada teks ASCII dengan gabungan huruf, angka, dan simbol, sehingga menghasilkan sebuah teks bersandi atau ciphertext berupa simbol-simbol berdasarkan tabel ASCII. Selanjutnya dilakukan pengujian Avalanche Effect, BER, CER, dan Entropi dengan hasil sesuai Gambar 9 hingga Gambar 12 secara berturut-turut.

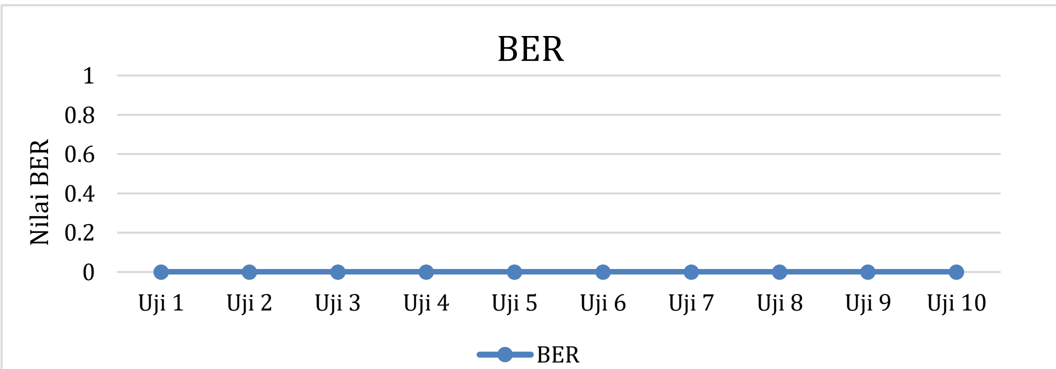


Gambar 9 Hasil Pengujian Avalanche

Berdasarkan Gambar 9, hasil nilai Avalanche Effect dari 10 pengujian yang sudah dilakukan rata-rata bernilai 50% ke atas, artinya Avalanche Effect yang dihasilkan menggunakan metode Vigenere Cipher bernilai baik. Penggunaan teks ASCII 256 dengan gabungan antara huruf, angka, dan simbol juga menambah tingkat keamanan informasi yang dihasilkan dari penggunaan metode Vigenere Cipher. Gambar 10 menunjukkan hasil pengujian Bit Error Rate (BER) dari hasil proses enkripsi yang telah dilakukan dalam pengujian sebelumnya. Nilai BER yang dihasilkan dari semua pengujian adalah 0 (nol). Hasil tersebut dikatakan baik karena, pengujian BER yang baik adalah jika nilai yang dihasilkan mendekati 0 (nol). Dimana hal tersebut menunjukkan bahwa tidak ada perbedaan antara plaintext dengan ciphertext yang dihasilkan.

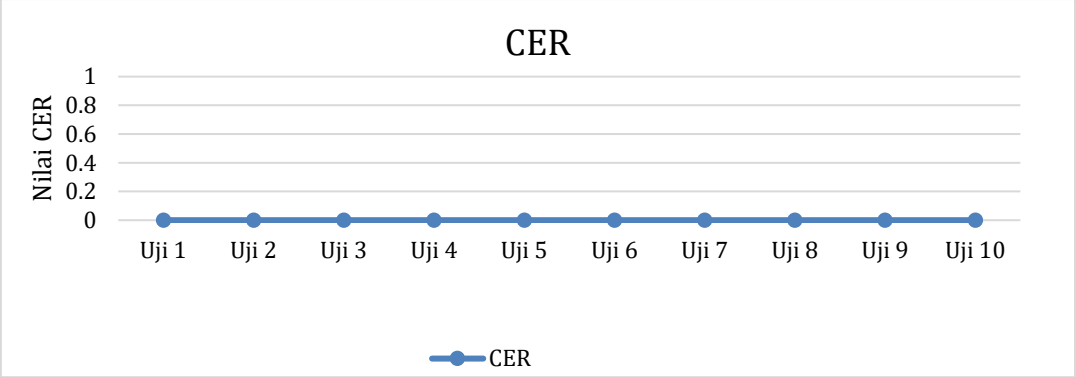
Tabel 1 Hasil Pengujian dengan Metode Vigenere Cipher

No.	Plaintext	Key	Chipertext
1	Universitas Dian Nuswantoro	!Polke_23	w¿ÙãÑØÓö¢Ä±ÕÇÎSÄ¸çÎÚÚÏ¥£
2	Mahasiswa Angkatan Tahun 2021	!Polke_23	o²ØÎßÏÓª•BÞÔ×ÇÔ¢"B¥ÑÕáÔ€dT,
3	Kriptografi_4312 Kelas Pagi	!Polke_23	mÃÙÝàÕÇ¥º•Ï¡Ÿ•½Ñà¶ÉÁš
4	Fakultas Ilmu Komputer Oke!!	!Polke_23	h²ÛâØÚÁ¦Tk½ÝâŒÏ ¤ÅÕßµËÜC
5	Teknik_Informatika_21_Polke!	!Polke_23	v¶ÛÛÕÑ¿|¢ÀâÚÍÚÉ¿Ì¼ÕÌ£™
6	Mata Kuliah Kriptografi 4312 kelas Kamis kagi lolos Free UTS semester_5 tahun 2023 Semangat!!	!Polke_23	o²äÎŒÕ¶Ÿ•ÞÏÐ§£‰ÃÑÓÕ¦eTqÛÒØÇÓS•¾Ù àÑ€ÁßB½ßÙÛÙ€¦‡ ¶•ÂÀ¹€¶™áÑØ¿hT²ØâÚ¢fUqÃÒÙÇÎš'
7	Universitas Dian Nuswantoro (Udinus) Fakultas Ilmu Komputer Prodi Teknik Informatika Angkatan 2021 Polke!	!Polke_23	w¿ÙãÑØÓö¢Ä±ÕÇÎSÄ¸çÎÚÚÏ¥£ByÅÑÕÔ Õ¦]BÑØáÒÔ" §BšÜÚá‹¢¡'ÆäÒÞº¶¥£¶•ÁÑÑÎ§ßÞÓÛØÍ"¼Ñ• -ÔÇžÞž TrÀÜØÑ‡
8	Universitas Dian Nuswantoro adalah Perguruan Tinggi Swasta atau PTS terbaik nomor satu di Semarang Jawa Tengah Indonesia	!Polke_23	w¿ÙãÑØÓö¢Ä±ÕÇÎSÄ¸çÎÚÚÏ¥£B²ÔÎØÇÈ S‡Ã×âÞÛÁ¡TvºÞÔÓÏ€ÄäÎÇÈÔ"©B¡ÄÀÚ€Å¥º ÛÚÕÍ¢¦BÄÑáá¶ÄŒu¶ÝÎÞÇÎšT²çÎºÅ¡¹¶ÚÊÏ¡º• Ñ
9	Sandi Vigenere adalah sandi substitusi polialfabet yang merupakan matriks 26 dengan 26 pergeseran sandi Caesar.	!Polke_23	u²ÞÑÕ¶¦¢ÕßÑÁŽØ•ßÇÎ•BÄåÏßÚÉ§©º•ÝÒÉ" ²ÒÒà¦Ù¢"‰ÝÒÞÛÐŸ¿ÚÍÚÒŸ¶¢£ÊÅ¡¿¶Ÿ¦Ð¦‰ãÒ ÞÇÎS§¿ÔÖŒÁ§Ãž
10	Udinus (UNIVERSITAS DIAN NUSWANTORO) mata_kuliah $Kriptografi kelas 4312 tahun2023 fre3 UTS & UAS 100% bis4 s3mangat!! ^0^	!Polke_23	wµÙÛáÙ€[%ÆE²¾¹©‡uq´¶-´€‰±»Àµ²]B¾ÑáÍ ÅË¨²Ø•±ÒœÀ×ßÍÎÉS¥½Ñà¶ËfBÅÑÕáÔ¢fUq ÖßÑ€™qÁ§³SeRÎ•ÏÓgT¸ÝÎÚÍÁ§UCqÎ•Ê

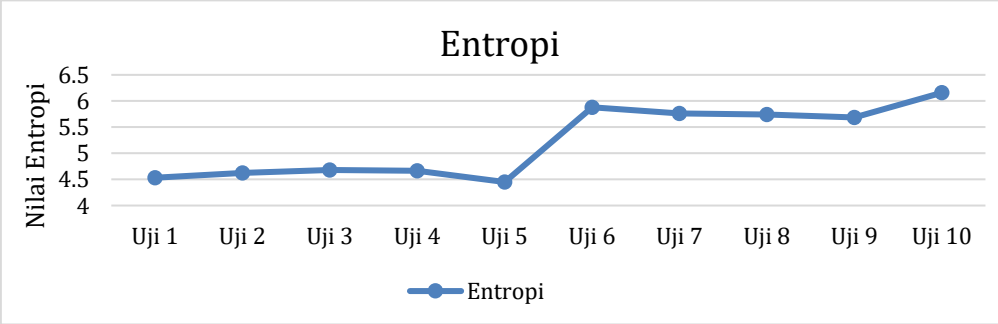


Gambar 10 Hasil Pengujian Bit Error Rate (BER)

Gambar 11 menunjukkan hasil pengujian Character Error Rate (CER). Berdasarkan Grafik 3, nilai CER yang didapat dari pengujian seluruhnya adalah 0 (nol), hal ini menunjukkan bahwa hasil enkripsi pada pengujian yang telah dilakukan memiliki tingkat akurasi yang tinggi. Dalam pengujian CER, hasil yang baik ditunjukkan jika nilai CER yang dihasilkan semakin rendah, dimana semakin rendah nilai CER maka semakin baik ciphertext yang dihasilkan.



Gambar 11 Hasil Pengujian Character Error Rate (CER)



Gambar 12 Hasil Pengujian Entropi

Pada Gambar 12 diketahui bahwa rata-rata hasil pengujian entropi yang dihasilkan bernilai 4 sampai 6 ke atas. Entropi bernilai 6 ke atas dihasilkan dari plaintext yang cukup panjang dan merupakan gabungan antara huruf, angka, dan simbol. Sedangkan, entropi bernilai di bawah 6 dihasilkan dari plaintext pendek yang hanya terdiri dari huruf saja, maupun gabungan antara huruf, angka, dan simbol. Hal ini menunjukkan bahwa panjang plaintext dan gabungan antara huruf, angka dan simbol dapat mempengaruhi besar nilai entropi yang dihasilkan. Entropi dikatakan baik jika nilainya mendekati 7.

4 Kesimpulan

Kesimpulan yang dapat diambil berdasarkan penelitian ini adalah Vigenere cipher adalah algoritma kriptografi substitusi. Kriptografi substitusi merupakan teknik yang merubah plainteks dengan cipherteks berdasarkan kunci. Selain mudah dalam pengimplementasianya juga memiliki kelebihan antara lain yaitu Vigenere Cipher termasuk kedalam polialfabetik cipher yang berarti setiap huruf pada plaintext dapat dienkripsikan menjadi huruf yang berbeda dalam ciphertext (berfokus pada frekuensi huruf). Vigenere cipher juga mampu mengatasi kelemahan utama Caesar Cipher, yaitu pola yang konsisten dalam pengaplikasian enkripsinya. Pada penelitian ini yang telah dilakukan metode Vigenere Cipher mendapatkan hasil rata-rata nilai Avalanche Effect yang baik dengan nilai diatas 50% menunjukan bahwa menggunakan metode Vigenere Cipher dapat menyandikan pesan dengan baik serta pengubahan panjang pesan (plaintext) dan kunci (key) dapat mempengaruhi Avalanche Effectnya.

Daftar Pustaka

[1] Marchandi and Ferdiansyah, "Implementasi Algoritma Vigenere Cipher Dalam Aplikasi Chatting Untuk Pengamanan Informasi Berbasis Desktop," *Skanika*, vol. 1, no. 1, pp. 340–345, 2018.

[2] D. A. Sitepu, "Implementasi pengamanan data menggunakan algoritma Advanced Encryption Standart (AES)," *J. Ilm. Kaputama*, vol. 6, no. 1, pp. 49–58, 2022.

[3] S. Azura *et al.*, "Penerapan Kemanan Data Text menggunakan Metode Kriptografi Vigener Chiper Berbasis Web," *Digit. Transform. Technol. | e*, vol. 3, no. 1, pp. 20–28, 2023.

[4] D. R. I. M. Setiadi, A. E. Handoyo, E. H. Rachmawanto, C. A. Sari, and A. Susanto, "Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA," *J. Teknol. dan Sist. Komput.*, vol. 6, no. 1, p. 37, Feb. 2018.

[5] E. H. Rachmawanto and C. A. Sari, "Keamanan File Menggunakan Teknik Kriptografi Shift Cipher," *Techno.COM*, vol. 14, no. 4, pp. 329–335, 2015.

[6] C. A. Sari and W. S. Sari, "Kombinasi Least Significant Bit (LSB-1) Dan Rivest Shamir Adleman (RSA) Dalam Kriptografi Citra Warna," vol. 13, no. 1, pp. 45–58, 2022.

[7] C. A. Sari and E. H. Rachmawanto, "Penyembunyian Data Untuk Seluruh Ekstensi File Menggunakan Kriptografi Vernam Cipher dan Bit Shiffting," *J. Appl. Intell. Syst.*, vol. 1, no. 3, pp. 179–190, 2016.

[8] E. H. Rachmawanto and C. A. Sari, "Gabungan Advanced Encryption Standard Dan Vigenere Cipher Untuk Pengamanan Dokumen Digital," *J. Inform. Polinema*, vol. 8, no. 4, pp. 1–8, 2022.

[9] T. Zebua and E. Ndruru, "Pengamanan Citra Digital Berdasarkan Modifikasi Algoritma RC4," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 4, no. 4, pp. 275–282, 2017.

[10] N. E. Saragih, "Implementasi Algoritma One Time Pad pada Pesan," *J. Ilm. MATRIK*, vol. Vol.20 No., no. 3, pp. 31–40, 2018.

[11] L. B. Handoko and C. Umam, "Kombinasi Vigenere-Aes 256 dan Fungsi Hash Dalam Kriptografi Aplikasi Chatting," *Pros. Sains Nas. dan Teknol.*, vol. 12, no. 1, p. 390, Nov. 2022.

[12] R. A. Megantara and F. A. Rafrastara, "Super Enkripsi Teks Kriptografi menggunakan Algoritma Hill Cipher dan Transposisi Kolom," *Pros. SENDI_U 2019*, pp. 85–92, 2019.

[13] D. K. Maulana, S. M. Tanjung, R. S. Ritonga, and A. Ikhwan, "Penerapan Kriptografi Vigenere Cipher Pada Kekuatan Kata Sandi," *J. Sains dan Teknol.*, vol. 3, no. 1, pp. 47–52, 2023.

[14] H. Touil, N. E. Akkad, and K. Satori, "Text Encryption: Hybrid cryptographic method using Vigenere and Hill Ciphers," in *2020 International Conference on Intelligent Systems and Computer Vision (ISCV)*, 2020, pp. 1–6.

[15] R. Rahim *et al.*, "Combination Vigenere Cipher and One Time Pad for Data Security," *Int. J. Eng. Technol.*, vol. 7, no. 2.3, pp. 92–94, 2018.

[16] D. Arfandy, M. Simanjuntak, and T. Pasaribu, "Penerapan Metode Vigenere Cipher Untuk Mengamankan Data Text," *JUKI J. Komput. dan Inform.*, vol. 4, no. 1, pp. 48–54, 2022.

[17] I. W. Utomo, R. Latifah, and R. D. Risanty, "Aplikasi Kriptografi Berbasis Android Menggunakan Algoritma Caesar Cipher & Vigenere Cipher," *J. Sist. Informasi, Teknol. Inf. dan Komput.*, vol. 9, no. 2, pp. 142–149, 2019.

[18] A. Rachmadsyah, A. Perdana, and A. Budiman, "Kombinasi Algoritma Beaufort Cipher dan Vigenere Cipher untuk Pengamanan Pesan Teks Berbasis Mobile Application," *J. Minfo Polgan*, vol. 9, no. 2, pp. 12–17, 2020.

[19] A. Susanto, D. R. I. Moses Setiadi, E. H. Rachmawanto, C. A. Sari, R. R. Ali, and I. U. Wahyu Mulyono, "Dual Security Method for Digital Image using HBV Encryption and Least Significant Bit Steganography," *J. Phys. Conf. Ser.*, vol. 1201, no. 1, p. 012024, May 2019.

[20] S. D. Nasution, G. L. Ginting, M. Syahrizal, and R. Rahim, "Data Security Using Vigenere Cipher and Goldbach Codes Algorithm," *Int. J. Eng. Res. Technol.*, vol. 6, no. 01, pp. 360–363, 2017.

[21] D. Sinaga, C. Umam, D. R. I. M. Setiadi, and E. H. Rachmawanto, "Teknik Super Enkripsi Menggunakan Transposisi Kolom Berbasis Vigenere Cipher Pada Citra Digital," *Din. Rekayasa*, vol. 14, no. 1, p. 57, 2018.

[22] A. A. Permana and D. Nurnaningsih, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes)," *J. Tek. Inform.*, vol. 11, no. 2, pp. 177–186, 2018.

[23] I. Prihandi, I. Ranggadara, S. Dwiasnati, Y. S. Sari, and Suhendra, "Implementation of Backpropagation Method for Identified Javanese Scripts," *J. Phys. Conf. Ser.*, vol. 1477, no. 3, 2020.

[24] S. A. Zebua, "Modifikasi Algoritma Vigenere Cipher dengan Pembangkit Kunci Random Number Generator Dalam Pengamanan Citra Digital," *J. Comput. Informatics Res.*, vol. 1, no. 3, pp. 71–81, 2022.

[25] N. B. Putra, B. C. Andika, A. D. P. Bagas, and M. Ridwan, "Implementasi Sandi Vigenere Cipher Dalam Mengenkripsikan Pesan," *J. JOCOTIS - J. Sci. Inform. Robot.*, vol. 1, no. 1, pp. 42–50, 2023.

[26] S. Sugiyanto and R. K. Hapsari, "Pengembangan Algoritma Advanced Encryption Standard pada Sistem Keamanan SMS Berbasis Android Menggunakan Algoritma Vigenere," *J. Ultim.*, vol. 8, no. 2, pp. 131–138, 2017.

[27] J. P. Sermeno, K. A. S. Secugal, and N. E. Mistio, "Modified Vigenere cryptosystem: An integrated data encryption module for learning management system," *Int. J. Appl. Sci. Eng.*, vol. 18, no. 4, pp. 1–10, 2021.

[28] A. Subandi, M. S. Lydia, R. W. Sembiring, M. Zarlis, and S. Efendi, "Vigenere cipher algorithm modification by adopting RC6 key expansion and double encryption process," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 420, no. 1, p. 012119, Oct. 2018.

[29] A. Salam, D. R. I. M. Setiadi, E. H. Rachmawanto, and C. A. Sari, "ShiftMod Cipher: A Symmetrical Cryptosystem Scheme," in *2019 International Seminar on Application for Technology of Information and Communication (iSemantic)*, 2019, pp. 1–5.

[30] H. K. R. Cahyono, C. A. Sari, D.R.I.M. Setiadi, and E. H. Rachmawanto, "Dual protection on message transmission based on Chinese remainder theorem and rivest cipher 4," in *2019 International Conference on Information and Communications Technology, ICOIACT 2019*, 2019.